

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

IN THE MATTER OF THE SEARCH OF
ONE MOBILE DEVICE CURRENTLY
STORED BY HOMELAND SECURITY
INVESTIGATIONS AT [REDACTED]

[REDACTED] HIS DEVICE IS DESCRIBED IN
FURTHER DETAIL BELOW

MJ-

24-144-B

FILED UNDER SEAL

SEARCH WARRANT AFFIDAVIT

I, Matthew Chakwin, being duly sworn, states:

INTRODUCTION

1. I, Matthew J. Chakwin, am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 of the United States Code, who is empowered by law to conduct investigations of, and to make arrests for, the offenses enumerated in Section 2516 of Title 18 of the United States Code.

2. I am a Special Agent and currently employed by Homeland Security Investigations ("HSI") and have been a federal law enforcement officer since April 2009. My formal education includes a Bachelor of Science Degree in Criminal Justice Studies from Georgia State University. From April 2009 until September 2009, I attended the Federal Law Enforcement Training Center ("FLETC"). During the course of my formal training at FLETC, I learned the fundamentals of how to conduct criminal investigations.

3. I am currently assigned to the Resident Agent in Charge Office of Mobile, Alabama, and am charged with investigations relating to organizations that utilize aircraft, boats, cars and other means to smuggle or traffic weapons, drugs, currency, contraband or that use these means to provide logistical support for their illicit operations. I am also involved with investigations related to drug trafficking through and around seaports of entry, fraud, and other

crimes involving persons and property. I have participated in the investigation of various drug trafficking organizations ("DTOs") involved in the acquisition, importation, transportation and distribution of controlled substances into and through the Southern District of Alabama. As the nature of my ongoing work at HSI requires that I keep abreast of recent trends and developments involved in the investigation of DTO's, I also speak with agents from the Drug Enforcement Administration ("DEA"), United States Border Patrol ("USBP"), Customs and Border Protection ("CBP") and various other local law enforcement officers operating within the Southern District of Alabama.

4. As a law enforcement officer since 2009, I have been involved in numerous financial and fraud investigations as either the lead case agent or assisting with the investigation. I have received extensive training and field experience in interview techniques and evidence collection.

5. By virtue of my employment as a Special Agent with HSI, I have performed or been trained in various tasks, which include, but are not limited to (a) providing surveillance, by observing and recording movements of persons trafficking in controlled substances and those suspected of trafficking in controlled substances; (b) tracing currency and assets gained by fraud, the laundering of monetary instruments, and other unlawful activity; (c) interviewing witnesses, cooperating individuals, and informants relative to the illegal trafficking of controlled substances; and (d) functioning as a case agent, which entails the supervision of specific investigations involving the trafficking of narcotics and the laundering of monetary instruments. I have been trained in investigations involving money laundering and wire fraud.

6. In furtherance of the financial crime and cybercrime investigations I have conducted or participated in, I have employed both traditional and contemporary investigative techniques to include physical surveillance, document review, witness interviews, record checks,

and the seizure and analysis of electronic media and data. I have also either led or participated in the execution of numerous search warrants, many of which involved the seizure of both tangible items of evidentiary value and electronic media and data.

7. As a Special Agent, I have conducted or been involved in financial fraud and cybercrime investigations, to include violations of Title 18, United States Code, Section 1791 (Possession of a Prohibited Item by an Inmate) committed by Adrian LACEY. I have received training at the Federal Law Enforcement Training Center regarding financial fraud and cybercrime, and I have attended specialized training courses in the areas of financial crime and money laundering during my career. In furtherance of the financial crime and cybercrime investigations I have conducted, I have employed both traditional and contemporary investigative techniques to include physical surveillance, document review, witness interviews, record checks, and the seizure and analysis of electronic media and data. I have also either led or participated in the execution of numerous search warrants, many of which involved the seizure of both tangible items of evidentiary value and electronic media and data.

8. This Affidavit is made in support of an application for a warrant to search the contents of one contraband mobile electronic device ("the device") that was confiscated by the Escambia County, Alabama Detention Center from Unit 5, occupied by Adrian LACEY on May 16, 2024. While no reasonable expectation of privacy exists for a contraband cellular device possessed contrary to law within a correctional facility, I am seeking a Search Warrant out of an abundance of caution and to establish probable cause that the devices now contain recoverable data that is evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and property designed for use, intended for use, or used in committing a crime.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

9. The property to be searched is described as follows:

A Black Samsung Cell Phone (IMEI 357532324348854) confiscated on May 16, 2024, which was recovered from the shower area after being placed there by Adrian LACEY, within the Escambia County Detention Center in Brewton, Alabama (the "Device").

10. The applied-for warrant would authorize the forensic examination of the device for the purpose of identifying electronically stored data particularly described in Attachment B. I have not included every fact known to me regarding this investigation, but only those facts and circumstances I believe are necessary to establish probable cause to show that the devices now in the lawful possession of HSI were prohibited objects possessed in violation of Title 18, United States Code, Section 1791, and therefore were evidence, fruits, and/or property designed for use, intended for use, or used for that crime.

11. In my training and experience, I know that the device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as when the device first came into the possession of the Escambia County Detention Center Officials and HSI.

APPLICABLE CRIMINAL LAWS

12. Title 18, United States Code, Section 1791 states in relevant part:

(a) Offense. Whoever— . . . (2) being an inmate of a prison, makes, possesses, or obtains, or attempts to make or obtain, a prohibited object; shall be punished as provided in subsection (b) of this section.

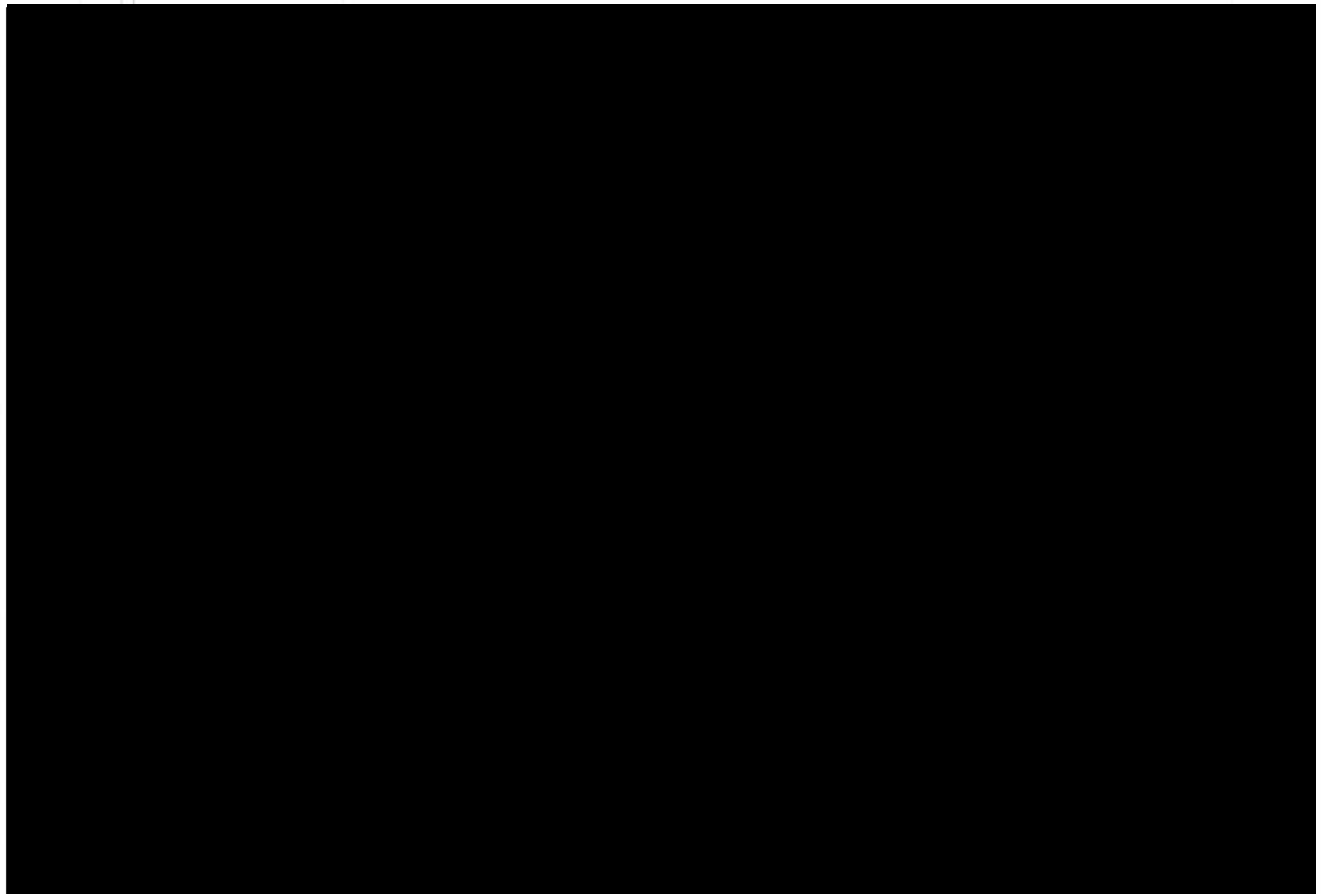
(b) Punishment. The punishment for an offense under this section is a fine under this title or— . . . (4) imprisonment for not more than one year, or both, if the object is specified in subsection (d)(1)(D), (d)(1)(E), or (d)(1)(F) of this section[.]

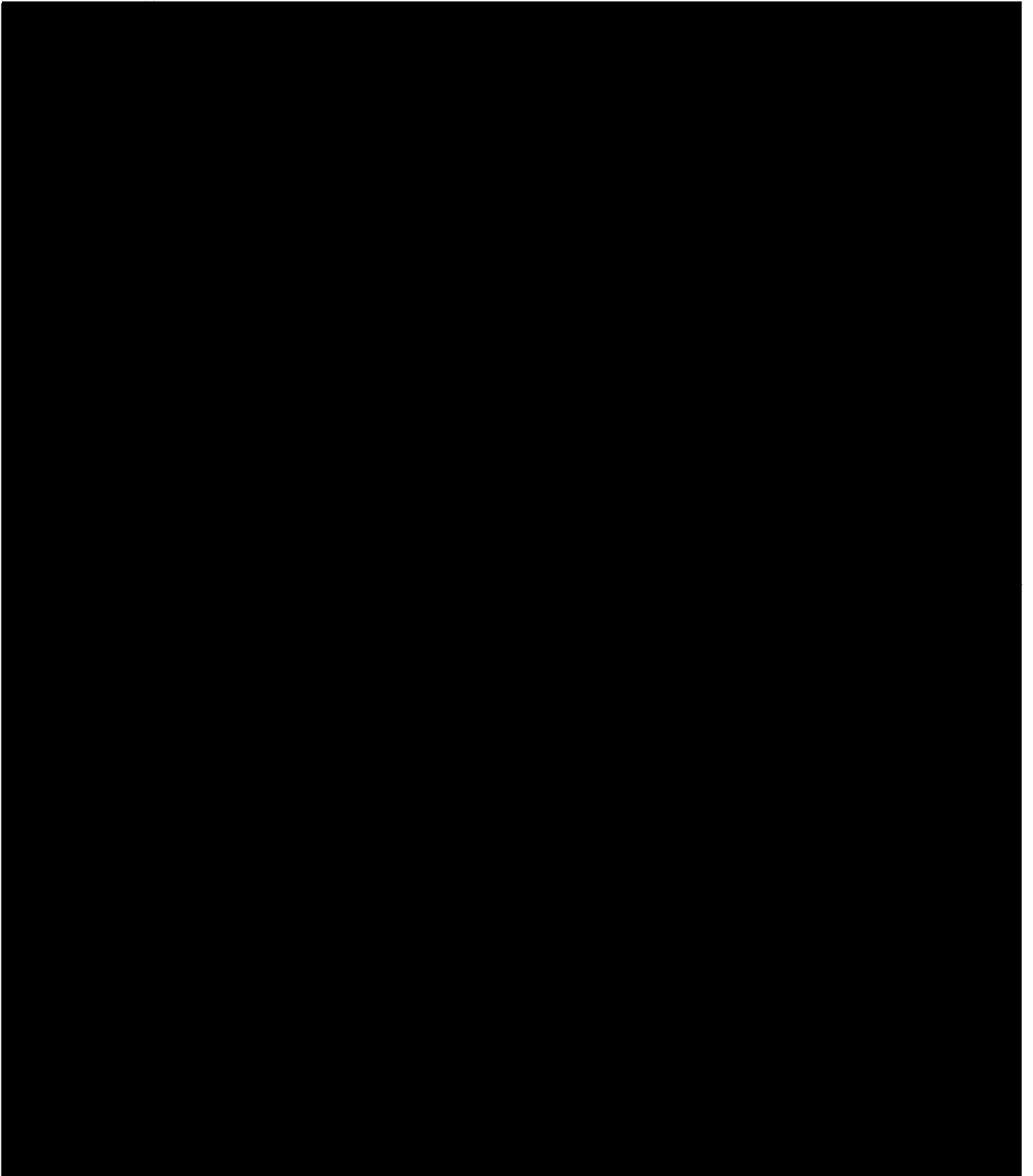
...
(d) Definitions. As used in this section—(1) the term "prohibited object" means— . . . (F) a phone or other device used by a user of commercial mobile service (as defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d))) in connection with such service[.] [And] (4) the term "prison" means a Federal correctional, detention, or penal facility or any prison, institution, or

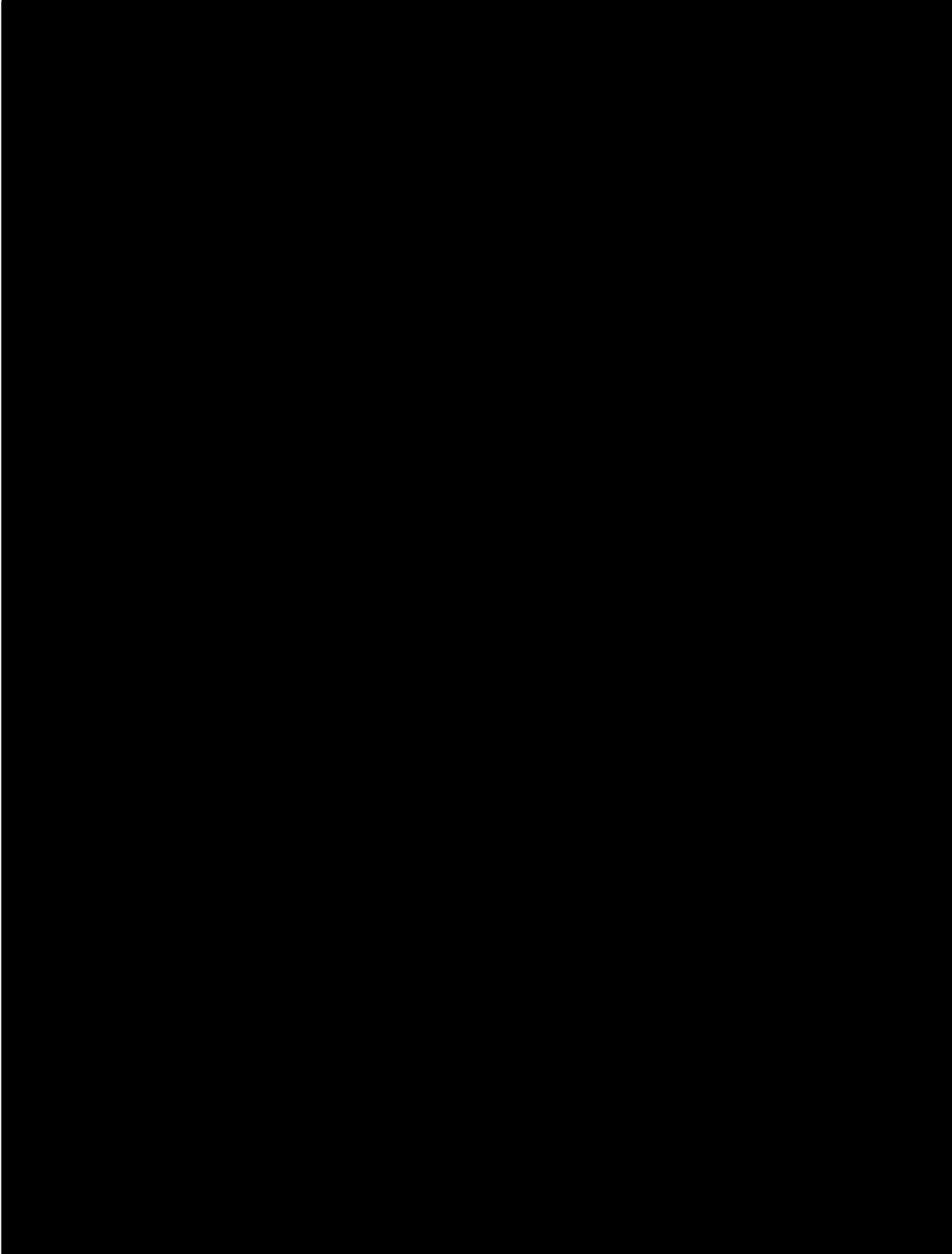
facility in which persons are held in custody by direction of or pursuant to a contract or agreement with the Attorney General.

13. I am requesting authority to search the device for the limited purpose of locating stored communications, documents, images, videos, and other electronic data and information as described in Attachment B related to the instant investigation involving the possession of a prohibited object and the ownership, control, and dominion over same. Because this Affidavit is submitted for the limited purpose of securing a search warrant, I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 1791 are now present and establish probable cause to search the identified device.

OVERVIEW OF INVESTIGATION







SEARCHES OF ELECTRONIC DEVICES

19. Smartphones, computers, and computer technology have revolutionized the way in which individuals conduct personal and official business, as well as how persons interact with each other. Electronic data storage devices are able to hold large volumes of data that would normally require large physical storage containers for papers, documents, ledgers, pictures, books, etcetera. Whereas business records were previously maintained in tangible paper form, electronic data storage allows individual users and business to operate on an almost paperless basis. The development of computers has changed this. Computers basically serve four functions in connection with business records: production, communication, distribution, and storage.

20. Criminals can now transfer documents, photographs, and other media onto a computer-readable format with a device known as a scanner. Today, applications available for download onto a smartphone at no cost allow the user to use their smartphone to create a .pdf file within seconds. These images can then be manipulated and edited, and/or transferred to other electronic devices or users via text message or email transmission for follow-on manipulation. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute legitimate, altered, or forged business documents. There is added benefit to the user that this method of production does not leave as large a trail for law enforcement to follow as other methods, commonly known as a "paper trail."

21. The ability of small electronic devices, such as smartphones, laptop computers, and desktop computers to store documents in digital form makes the computer itself an ideal repository for legitimate and fraudulent business documents. Like a locked file cabinet, modern electronic

devices offer encryption and password protection, with some now even utilizing facial recognition, in order to prevent unwanted, unwelcome, or law enforcement access to data. The size of the electronic storage media (commonly referred to as the hard drive) used in laptop and desktop computers has grown tremendously within the last years. It is only with careful laboratory examination of electronic storage devices that it may be possible to recreate the evidence trail.

22. Another method which technologically savvy criminals utilize to store evidence, fruits, and instrumentalities of their crimes include an external hard drive, commonly known as a pen drive, thumb drive, cruiser disk or USB drive. Such drives can be physically small in nature but have the capacity to store thousands of electronic documents, images, and audio/visual media. The small size of the drives makes them compact and mobile in addition to making them easy to conceal.

23. Criminals are also known to use cellular telephones, regularly identified in the common vernacular as "smartphones," and other cellular communications devices for the purpose of storing, preserving, and distributing evidence of their crimes. Although, these mobile devices are small in size, some are capable of storing extremely large amounts of data. I believe that the organization of which Adrian LACEY is the apparent leader uses personal cellular devices, and that these items represent instrumentalities used to commit the underlying offenses.

24. Internet Protocol (IP) addresses, expressed as a series of numbers or alphanumeric combinations separated by decimal points or colons, are used to definitively identify a particular computer on the Internet. When a computer user visits a website on the Internet, their IP address is visible to that website. Law enforcement entities, in conjunction with Internet Service Providers, have the ability to identify a user's IP address to a specific household or residence.

SEIZURES AND CONTROLLED SEARCHES
OF ELECTRONIC DEVICES

25. Based on my own experience and my consultation with other agents who have been involved in searches of electronic devices, searching digital information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. I am familiar with and understand the implications of the Privacy Protection Act (PPA), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that the devices to be searched are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

UNLOCKING DEVICES WITH BIOMETRIC FEATURES

26. The warrant I am applying for would permit law enforcement to compel the custodian/owner of the device to unlock the devices subject to seizure pursuant to this warrant using the device's biometric features. I seek this authority based on the following:

- a. I know from my training and experience, as well as from information found in publicly available materials published by devices manufacturers, that many electronic devices, particularly newer mobile devices and tablets, offer their users the ability to unlock the devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the devices through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the devices by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the devices. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the devices through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the devices in front of his or her

face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the devices in front of his or her face. The devices then direct an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. The passcode or password that would unlock the devices subject to search under this warrant are not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices,

making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the devices was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked devices equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.


27. Due to the foregoing, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of the custodian/owner to the fingerprint scanner of the devices seized pursuant to this warrant; (2) hold the device found at the premises in front of the face the custodian/owner in order to activate the facial recognition feature; and/or (3) hold the device found at the premises in front of the faces of the same individual and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

CONCLUSION

28. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe violations of Title 18, United States Code, Section 1791 have been committed, and that evidence of those violations and information related to the identity/identities of the perpetrators is located within the devices. I submit that the device in HSI custody is an instrumentality of the crime that has occurred, and that the data contained in the devices will identify conspirators, fraud victims, and other items of crucial evidentiary value.

29. I respectfully submit that this evidence constitutes the instrumentalities and the fruits of crime or things otherwise criminally possessed, or property or contraband that is or has been used as the means of committing the foregoing offenses and is located within the devices. I respectfully request this Court for authority to search for and seize such material via the issuance of a search warrant for the devices more particularly described in Attachment "A" of this affidavit, authorizing the seizure of the items described in Attachment "B".

30. Accordingly, it is respectfully requested that the Court issue a warrant authorizing any authorized federal law enforcement agent or agency, in its discretion, to search for and seize evidence located within the device more particularly described in Attachment B.


Special Agent Matthew J. Chakwin
Department of Homeland Security
Homeland Security Investigations

THE ABOVE AGENT HAS ATTESTED
TO THIS AFFIDAVIT PURSUANT TO
FED. R. CRIM. P. 4.1(b)(2)(B) THIS 17th
DAY OF MAY 2024.


UNITED STATES MAGISTRATE JUDGE SONJA BIVINS

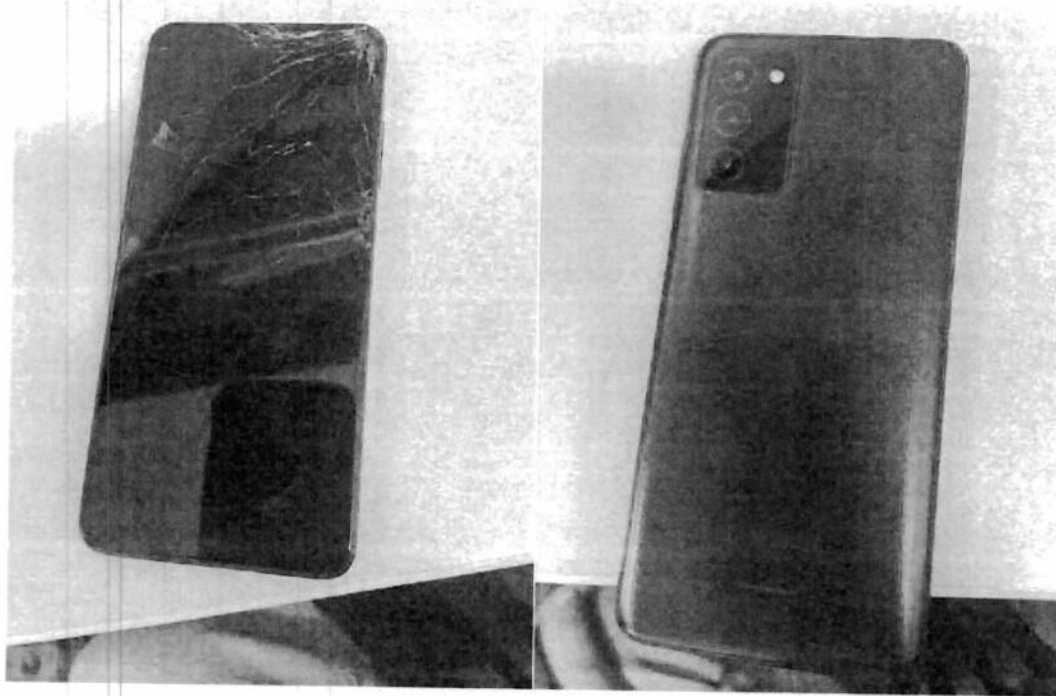
Attachment A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The property to be searched consists of:

A Black Samsung Cell Phone (IMEI 357532324348854) confiscated on May 16, 2024, which was recovered from the shower area after being placed there by Adrian LACEY, within the Escambia County Detention Center in Brewton, Alabama (the "Device").

The Subject Device is currently stored at the Homeland Security Investigations field office located at [REDACTED]. This warrant authorizes the forensic examination of the device for the purpose of identifying the electronically stored information described in Attachment B.



Attachment B

LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

